

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method for generating hierarchical keys of digital assets, encrypting the digital assets in a digital asset server, and utilizing the keys of the digital assets and the encrypted digital assets in an associated digital asset client, comprising the steps of:

5 digitizing and organizing lectures in an e-learning system to produce the digital assets

 arranging the digital assets in the digital asset server as at least one tree structure, a root node of the tree structure representing a complete set of the digital assets, other group nodes representing sub-sets in each level of the digital assets respectively, and the nodes in the lowest level being leaf nodes; wherein a text string identifying a node in the tree structure is generated by appending text to a text string identifying the node's parent node;

10

 randomly generating key of the root node in the digital asset server; starting with the key of the root node, using the key of a father node to compute level by level computed keys of its child nodes through to leaf nodes using a one way function, in the digital asset server; wherein the one way function is responsive to the text string identifying a node;

15

 encrypting corresponding digital assets in the digital asset server using the computed keys;

20 providing the one way function at the digital asset client either by communicating from the digital asset server to the digital asset client or by embedding the one way function at the digital asset client;

requesting an encrypted digital asset at the digital asset client,
and determining if a key for the requested encrypted digital asset is present on
25 the digital asset client;

if the digital asset key is not present on the digital asset client,
the digital asset client requesting the digital asset key from the digital asset
server;

the digital asset server receiver requests from the digital asset
30 client, and thereafter transmits a digital asset key, if requested, and a
requested encrypted digital asset from the digital asset server to the
associated digital asset client; and

receiving the key and the encrypted digital asset from the digital
asset server at the digital asset client and decrypting the encrypted digital
35 asset utilizing the key;

generating, at the digital asset client, keys for descendent nodes
of a group node, responsive to the group node's key and the one way function.

2. (Original) The method according to claim 1, comprising
computing different keys for two nodes having the same father node.

3. (Original) The method according to claim 1, comprising
computing different keys for child nodes having the same father node.

4-5. (Canceled)

6. (Previously Presented) The method according to claim 1,
comprising encrypting the corresponding digital assets using at least a part of
the generated node keys.

7. (Previously Presented) The method according to claim 6 comprising encrypting the digital assets using a cipher, and encrypting the cipher using at least a part of the generated node keys.

8. (Canceled)

9. (Currently Amended) An apparatus for managing digital assets consisting of digitized lectures in an e-learning system and hierarchical keys of the digital assets, comprising a digital asset server and a digital asset client:

5 said digital asset server comprising a central processor unit, a bus, and memory, and further comprising:

(a) a key tree management unit for arranging the digital assets as at least one tree structure for management, a root node of the tree structure representing the complete set of the digital assets, other group nodes
10 representing sub-sets in each level of the digital assets respectively, and the nodes in the lowest level being leaf nodes, said apparatus further comprises:

(b) a root node key generating unit for generating the key of the root node; and

(c) a first computing unit for starting with the key of the root node,
15 using the key of a father node to compute level by level the keys of its child nodes according to a predetermined one-way function, through to leaf nodes;

(d) an encrypting unit for encrypting the corresponding digital assets by using at least a part of the generated node keys;

(e) an input interface unit for accepting instructions from an
20 administrator; the instructions comprising: modifying the tree structure, changing content of the asset, regenerating a root key and computing a cipher key at a node;

wherein said root node represents a main course and said leaf nodes represent lectures in various courses; and

25 said digital asset client comprising a central processor unit, a bus, and memory, and further comprising:

(a) a second computing unit for requesting an encrypted digital asset from the digital asset server, searching for node keys stored on the digital asset client for the requested digital asset, and, computing the keys of the
30 nodes in lower levels of said node through to leaf nodes in turn; and

(b) a decrypting unit for decrypting the digital assets contained in all nodes by using the computed node keys of all nodes of the requested digital assets; wherein the decrypting unit generates keys for descendent nodes of a group node using the group node's key and the predetermined one-way
35 function.

10. (Canceled)

11. (Previously Presented) The apparatus according to claim 9, adapted for computing different keys for different nodes having the same father node.

12. (Canceled)

13. (Previously Presented) The apparatus according to claim 9, further comprising an encrypting unit for encrypting the digital assets first by using a cipher, and then encrypting the cipher by using at least a part of the generated node keys.

14-19. (Canceled)

20. (Currently Amended) A program product comprising media including a machine-readable data storage medium selected from the group consisting of magnetic hard drives, RAID arrays, RAMACs, a magnetic data storage diskettes, magnetic tape, digital optical tape, RAMs, ROMs, EPROMs, EEPROMs, and flash memories, having computer readable instructions written thereon for directing a computer to perform a process for generating hierarchical keys of digital assets and encrypting the digital assets in a digital asset server, and utilizing the keys of the digital assets and the encrypted digital assets in an associated digital asset client, comprising the steps of:

5 creating the digital assets by digitizing lectures;

10 arranging the digital assets in the digital asset server as at least one tree structure, a root node of the tree structure representing a complete set of the digital assets, other group nodes representing sub-sets in each level of the digital assets respectively, and the nodes in the lowest level being leaf

15 nodes;

 randomly generating, responsive to a text string identifying the root node, a key of the root node in the digital asset server; and

 starting with the key of the root node, using the key of a father node to compute level by level computed keys of its child nodes through to leaf

20 nodes using a one way function, in the digital asset server;

providing a one-way function from the digital asset server to the digital asset client;

checking by an authentication process if a digital asset client requesting an asset is a legal user of the asset;

25 accepting instructions from an administrator through an input interface; the instructions comprising one or more of: modifying the tree structure; adding, amending, or deleting asset contents; regenerating a root key; computing keys of various nodes at various levels; and encrypting modified asset content;

- 30 transmitting a key and an encrypted digital asset from the digital asset server to the associated digital asset client; and
- receiving the key and the encrypted digital asset from the digital asset server at the digital asset client and decrypting the encrypted digital asset utilizing the key.

21. (Original) The program product according to claim 20, said process comprising computing different keys for two nodes having the same father node.

22. (Original) The program product according to claim 20, said process comprising computing different keys for child nodes having the same father node.

23.-24. (Canceled)

25. (Previously Presented) The program product according to claim 21, said process comprising encrypting the corresponding digital assets using at least a part of the generated node keys or their deformation.

26. (Previously Presented) The program product according to claim 25 said process comprising encrypting the digital assets using a cipher, and encrypting the cipher using at least a part of the generated node keys.

27. (Canceled)